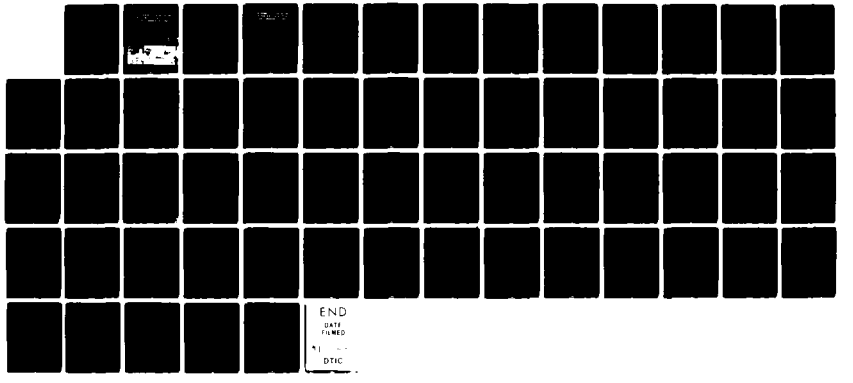
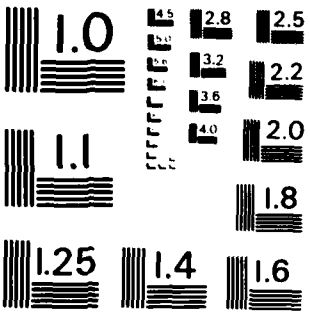
AD-A134 166 DEFENSE DATA NETWORK SYSTEM TEST FACILITY (STF) 1/1
RECOMMENDATIONS(U) COMPUTER SCIENCES CORP FALLS CHURCH
VA 09 SEP 83 CSC-DDN-TE-2 DCA100-78-C-0053

UNCLASSIFIED F/G 5/1 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS - 1963 - A

2

TECHNICAL REPORT DDN-TE-2

DEFENSE DATA NETWORK SYSTEM TEST FACILITY (STF) RECOMMENDATIONS

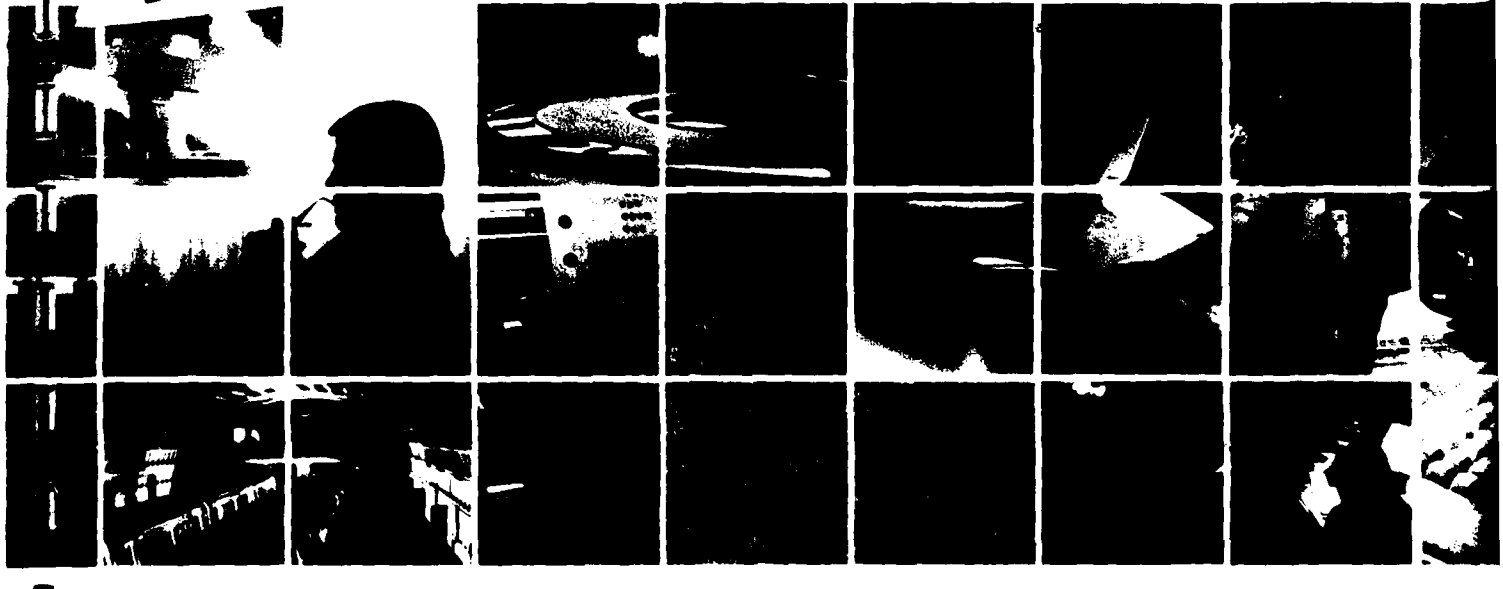
Prepared for

DEFENSE COMMUNICATIONS AGENCY
WASHINGTON, D.C.

Under

CONTRACT DCA100-78-C-0053
TASK 6-83

9 SEPTEMBER 1983



CSC
COMPUTER SCIENCES CORPORATION

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER DDN-TE-2	2. GOVT ACCESSION NO. AD-A134166	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* Defense Data Network System Test Facility Recommendations		5. TYPE OF REPORT & PERIOD COVERED Final Report June - Sept. 1983 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR*(s)*		8. CONTRACT OR GRANT NUMBER*(s)* DCA 100-78-C-0053
9. PERFORMING ORGANIZATION NAME AND ADDRESS Computer Sciences Corporation 6565 Arlington Blvd. Falls Church, VA 22046		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 33126K
11. CONTROLLING OFFICE NAME AND ADDRESS Defense Communications Engineering Center 1860 Wiehle Avenue, Code R110 Reston, VA 22090		12. REPORT DATE 9 Sept. 1983 13. NUMBER OF PAGES 53
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)*		15. SECURITY CLASS. *(of this report)* UNCLASSIFIED 15a. DECLASSIFICATION DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Defense Data Network
Test and Evaluation
Packet Switching
System Testing

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

This report identifies the required functional capabilities of the Defense Data Network System Test Facility. The necessary components of the DDN STF are identified and the recommended management structure described.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

TECHNICAL REPORT DDN-TE-2

DEFENSE DATA NETWORK SYSTEM TEST FACILITY (STF) RECOMMENDATIONS

Prepared for

DEFENSE COMMUNICATIONS AGENCY
WASHINGTON, D.C.

Under

CONTRACT DCA100-78-C-0053
TASK 6-83

9 SEPTEMBER 1983

Accession For	
NTIS GRA&I	X
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

COMPUTER SCIENCES CORPORATION

6565 Arlington Boulevard

Falls Church, Virginia 22046

Major Offices and Facilities Throughout the World

CONTENTS

CONTENTS
(Continued)

LIST OF ILLUSTRATIONS

EXECUTIVE SUMMARY

The DDN PMO is responsible for overall management of the DDN Program, including test and evaluation of network components, installation of network elements, and activation and deactivation of DDN DCS trunk lines.

This document identifies DDN System Test Facility (STF), required DDN functional capabilities, essential equipment, a test management structure, and an acquisition process to achieve these test capabilities. To provide definition of the STF, two requirements have been identified. The first requirement is to support development and acceptance testing of components to validate their performance, as well as to advance technology in support of DDN. Secondly, the STF must be able to simulate both network operation in a standalone configuration and to participate as a test node in network integration testing.

Primary issues include the precept that the DDN Program can be considered as modernization and expansion of the Defense Communications System and the several existing DoD networks. Previous network experience forms a baseline of capabilities, equipment, and facilities upon which to develop DDN test capabilities. A fully capable DDN STF requires close coordination and a sharing of resources such as those located in the Reston Communications Test Facility, the Experimental Data Network, the Command and Control Test Center, and the proposed DCEC/NBS Protocol Laboratory. Evolution of the DDN to its full potential requires extensive planning for the integration of existing or planned DoD networks. A comprehensive transition plan for network integration is essential to provide specific milestones for STF test scheduling.

To meet the challenge of this complex environment and to ensure sufficient resources to accomplish required testing, the following recommendations are made:

(a) A government-owned DDN System Test Facility tailored to DDN needs should be established.

(b) The STF should be of sufficient size and flexibility to allow various configurations to simulate any potential subnetwork or major component thereof.

(c) Use existing equipment and facilities to achieve preliminary test capability.

(d) Modest subnetwork and monitoring center functions should be made available to vendors on a controlled basis.

(e) A Test Planning Working Group made up of representatives of the several DoD networks should be formed to advise the DDN PMO and coordinate respective network test activities.

1. INTRODUCTION

1.1 Purpose. This report has been prepared in response to Defense Communications Agency (DCA) Task Order 6-83 issued under the terms and conditions of Contract DCA100-78-C-0053 as amended. It constitutes CDRL Line Item 002 of the Task Order. In accordance with the Statement of Work (SOW), its purpose is to analyze the test and evaluation actions recommended in CDRL Line Item 001 of the Task Order, develop alternatives, and provide a plan for the acquisition of a DDN Systems Test Facility (STF) and other capabilities necessary to implement the Test and Evaluation Recommendations.

1.2 Objective. The objective of this report is to provide information which is needed to develop a plan for the acquisition of a DDN System Test Facility (STF), facilities and/or capabilities necessary to implement the T&E recommendations of CDRL line item 001 to the Government in an easily accessible form. The requirement for a DDN STF acquisition plan and the information contained in this report stem from the following statements of need:

(a) The need to perform test and evaluation on the DDN component elements and subsystems to assure network performance.

(b) The need for Independent Verification, Validation, and Testing (IVV&T) of the critical software and firmware elements of the DDN.

(c) The need to develop a description of the functional capabilities required for DDN testing, and recommendations regarding the establishment of a DDN test facility or facilities.

This report provides the information necessary to meet these needs in a government-owned DDN STF. Its content is in accordance with the requirements of subtask 2 of the Task Description of Task Order 6-83.

1.3 Scope. AN environment for the support of DDN development, experimentation, and testing should be developed by the DDN PMO. To provide definition of the STF, two requirements have been identified. The first is to support development and acceptance testing of components to validate their performance as well as to advance technology in support of DDN. Secondly, the STF must be able to simulate both network operation in a standalone configuration and to participate as a test node in network integration testing. This report provides a description of required functional capabilities, hardware and software components, configurations, and management of the facility.

It is expected that the specific uses of the DDN STF in fulfilling the objectives defined in this report will be planned, programmed, and scheduled by the DDN System Test Director in coordination with the DDN Test Planning Working Group, as discussed in paragraph 3.3, and in accordance with specific needs for development and testing.

1.4 Assumptions.

(a) A transition plan for integration of the various subnetworks will be written to provide specific milestones on which to base testing schedules.

(b) The STF as a test and development facility will be supplemented by the Experimental ARPANET.

(c) The planned evolution of the DDN to a fully capable multilevel secure mainstay of the DCS will require testing facilities which are configured to the security posture required by appropriate directives.

(d) Certain security devices under development will be subjected to thorough T&E and IVV&T before being released to the DDN. Testing of these items by DDN will focus on their impact on network connectivity and performance.

(e) The BBN requirement for a developmental testing capability in order to fulfill current contracts is valid.

(f) The requirement for each subnetwork to retain its test facility and test bed configuration will remain valid in light of each subnetwork's requirement to support functional and substantive enhancements for subscribers in its Community of Interest.

(g) The crypto units identified in this report and anticipated for use in DDN are KG-84s; however, it is recognized that, over the life cycle of the DDN, newly developed cryptographic equipment may be used.

1.5 Methodology. The methodology for task completion is as shown in Figure 1-1.

1.6 Review of Subtask 1 Recommendations. A capability to test DDN network components (hardware, software, and especially IVV&T of software) is required. This requirement extends from early IVV&T of proposed software to government acceptance testing of components. Although site transition testing conducted prior to DDN network integration is fundamentally a subnetwork controller responsibility, it should be recognized that a great amount of coordination as well as test data will be required by the DDN PMO prior to subnetwork cutover to DDN. In the area of network integration testing, the DDN should have its own System Test Facility for network maintenance and enhancement, just as subnetworks now have their own test facilities for subnetwork maintenance and enhancement. Especially important is the requirement to test network interfaces and software protocols for Community of Interest (COI) and security separation.

1.7 Functional Capabilities of Existing T&E Facilities. Although not discussed as a separate topic within this report, the basic tenet of this report is that existing test and evaluation facilities are tailored to their specific subnetwork needs in terms of capability, manning, and management. Likewise, a DDN STF should be tailored to DDN needs (larger than an individual subnetwork) with emphasis on software protocol testing, host interface testing, and security testing, appropriately manned and managed by DDN personnel for ease of operation.

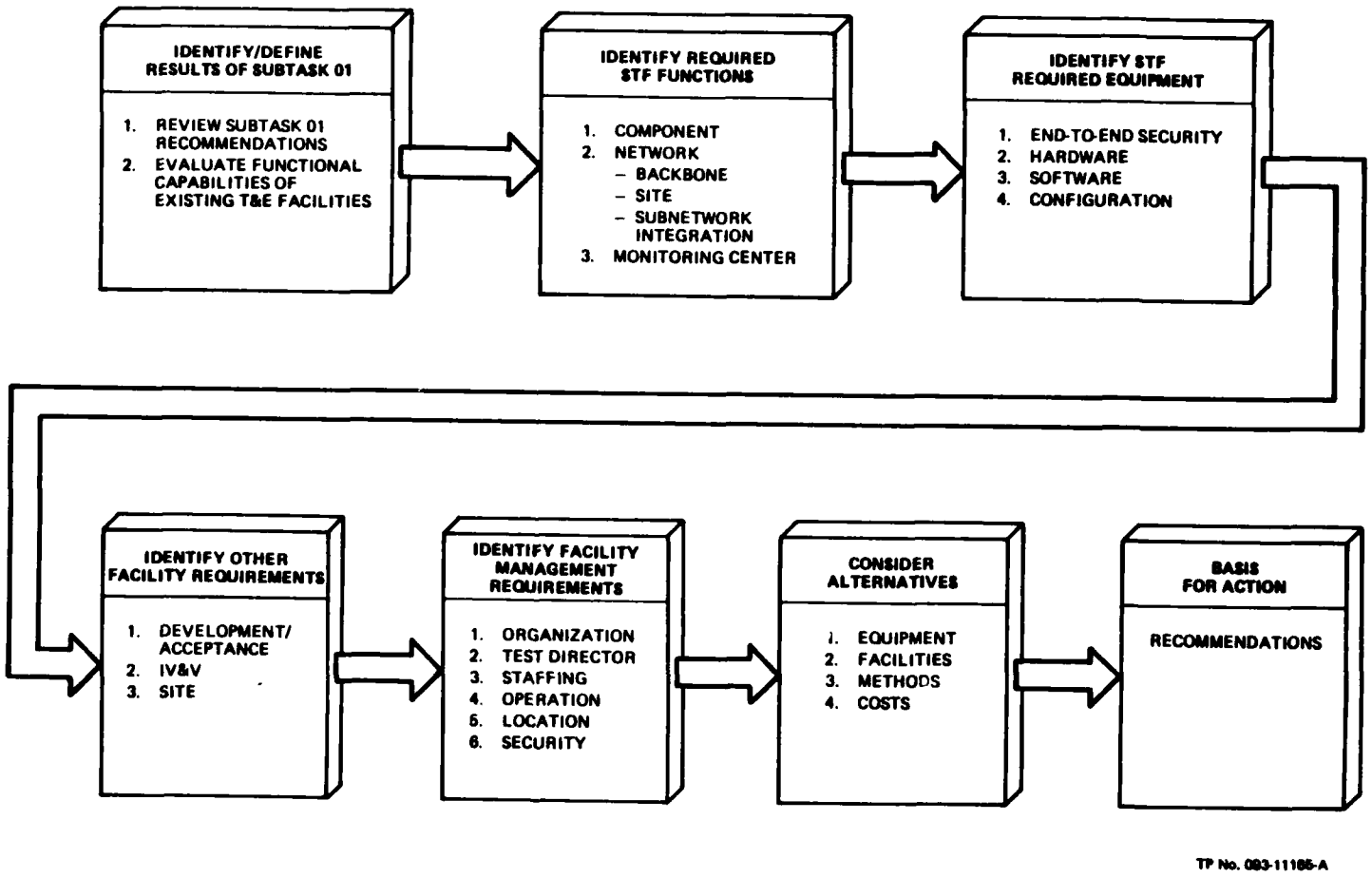


Figure 1-1. Task Approach

2. TEST AND EVALUATION REQUIREMENTS ANALYSIS

2.1 System Test Facility (STF) - Required Functional Capabilities. The requirement for an STF is predicated on the concept that the DDN PMO responsibilties include replicating problems and developing solutions to DDN problems, and testing and certifying the performance of:

(a) New data communications hardware, concepts and standards for DDN Backbone communications capabilities

(b) The DDN provided interfaces for sites or systems by Community of Interest (COI) subsystems joining DDN (validation of software releases)

(c) New software protocols to ensure that the interface characteristics are in conformance with DDN specifications

(d) DDN enhancements.

The DDN STF should be established in order to test within the prioritized list as shown below:

(a) Protocols
(b) Interfaces
(c) Security
(d) Network Integration Testing
(e) IVV&T
(f) Component acceptance testing
(g) Testing to determine satisfactory interoperability of DDN with other systems (user satisfaction).

The DDN STF must be capable of operating in two different modes. In the standalone, or nonintegrated network mode, the STF should be capable of duplicating and testing software and communication configurations associated with any of the networks existing in the DDN. Implicit in the standalone mode is the requirement to reconfigure to each of the subnetworks in order to duplicate each network of operation and level of security for

evaluation and performance testing. In the integrated mode, the STF should be capable of operating as one or more nodes in the operational DDN, in order to conduct certain types of network testing. In this mode, the facility should also be able to support operational contingencies with other organic equipment. When the STF is integrated as an operational node of the DDN, it must be capable of operating at the appropriate security level.

During the evolutionary development of the STF, before it is fully manned and operational, nonintegrated operation should be the day-to-day mode to fulfill standalone testing requirements according to the prioritized list above. When fully developed and manned on a schedule commensurate with overall DDN development and integration, the STF will normally operate in the integrated mode, but all or part of its capabilities will be used in the non-integrated mode when required.

2.1.1 Testing Capabilities. The STF configuration should be such that operational tests and formal acceptance testing of prototype and production hardware and software in a simulated DDN environment may be accomplished. A remote test capability is required to permit testing of new components at vendor locations or places other than the STF. This capability should work in both directions so that vendors have access to STF facilities for check-out and acceptance.

Five levels of testing have been considered for the DDN STF. As described in paragraphs (a)-(g) below, the levels of experimentation and testing apply to the use of the DDN STF for developmental testing, including performance evaluation in support of the DDN. The DDN STF should also be used to support other objectives such as testing of software releases. Levels of experimentation and testing may be combined in some cases; all levels are not likely to apply to any one development. Figure 2-1 illustrates the relationship among the levels.

(a) Baseline Establishment. This level of testing is conducted to establish or verify the relationship between a DDN STF standalone configuration and an actual

subnetwork configuration. Such testing is not limited to physical devices and software used, but may also include factors such as workload on a subnetwork, and types and characteristics of backbone communication paths.

(b) Feasibility and Applicability Assessment. This level of experimentation is conducted to determine the feasibility of including a particular technology (hardware or software) in a DDN environment, and to gain insight into the possibility of applying the technology to DDN. General determination of the feasibility and applicability is derived from the reactions of subscribers to the limited demonstration of the technology in a specific situation and environment simulated by the DDN STF. Favorable reaction to the preliminary demonstration leads to experimentation in a wider range of operating conditions to provide more complete information on compatibility of the technology with the DDN.

(c) Experimental Testing Tool and Application Development. This level of experimentation provides the support environment in which to develop management and testing tools for DDN performance evaluation. It includes use of appropriate DDN STF capabilities for software and hardware tools, as well as application development and developmental testing.

(d) Experimental Testing Tool and Application Validation. This level of experimentation is conducted to validate the compatibility of specific hardware or software tools or application with the DDN environment and to validate its compliance with technical specifications and performance parameters. It involves a variety of normal and abnormal operating conditions simulated by the DDN STF. Baselines established by previous testing are used

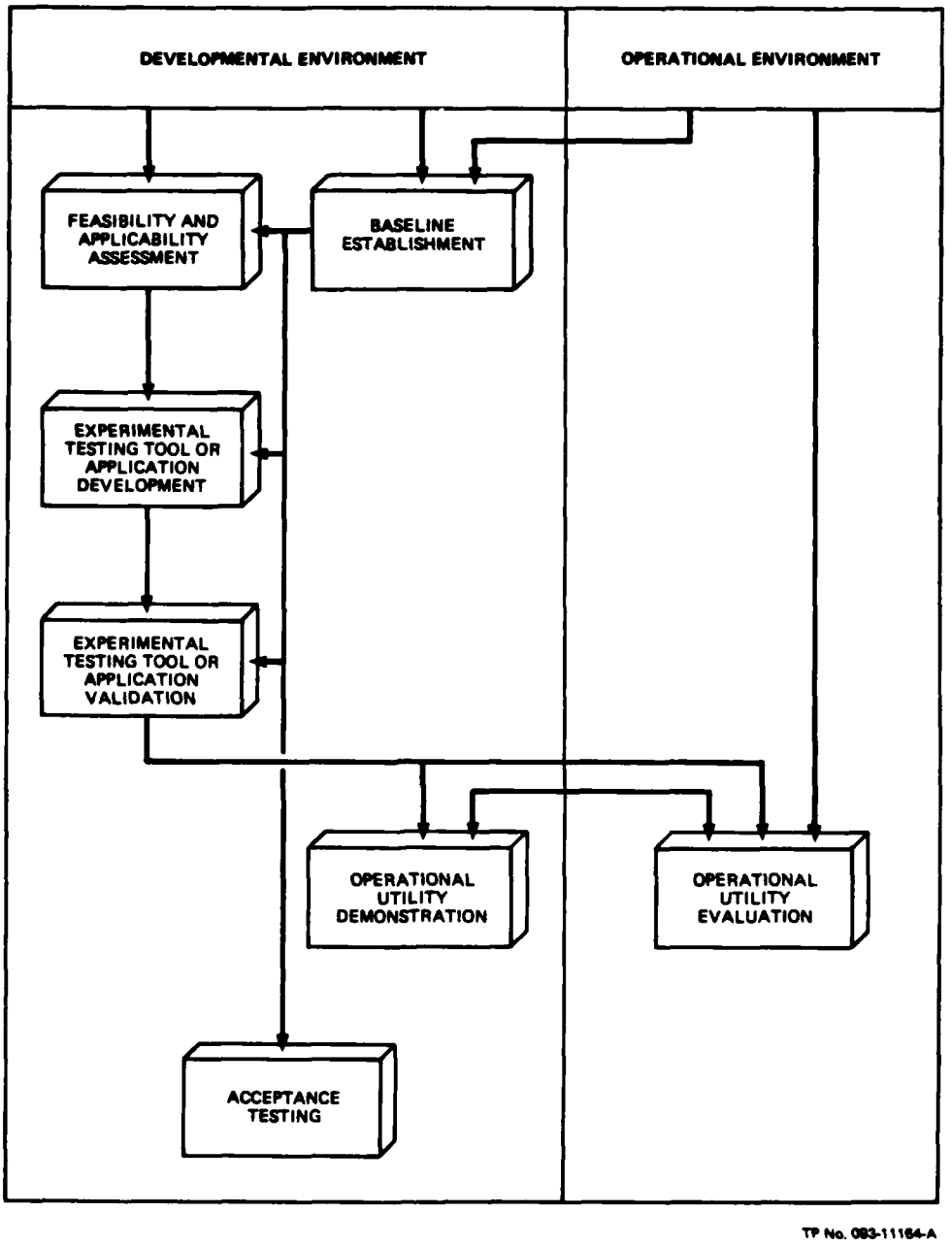


Figure 2-1. Relationships Among Levels of Experimentation and Testing

for comparison and as the basis for specific testing conditions. Workloads may be generated by DDN STF internal capabilities (refer to Table 2-1) rather than actual network subscribers.

(e) Operational Utility Demonstration. This level of testing is conducted to obtain subscriber reaction to a new DDN capability under less structured conditions than a formal operational utility evaluation, as discussed below. It involves use of newly validated technology for compatibility with DDN. DDN standalone capabilities are used to establish a realistic simulation of some portion of the DDN. DDN STF personnel exercise the new technology in representative situations. Evaluation consists of a combination of those measures of performance made during demonstration and the impressions of user personnel.

(f) Operational Utility Evaluation. This level of testing is conducted for formal measurement of the operational utility of a new technology that has been previously validated for DDN compatibility and for compliance with technical specifications. DDN STF capabilities are used to establish a realistic simulation of some portion of the DDN, including workloads, to exercise the new technology in representative situations. The DDN STF may be integrated with individual operational or prototype subscriber sites, or partitioned elements of an operational DDN subnetwork for operational utility evaluation, in order to provide realistic user involvement in the evaluation. Evaluation includes measurements of performance, effectiveness, and utility made under controlled conditions during testing. Formally established measures of utility are applied, which may include structured use of impressions of operational user participants.

(g) Acceptance testing. This level of testing is conducted to formally evaluate compliance of hardware and software components to established technical requirements. Acceptance testing may be conducted on internally developed capabilities, such as software releases, before they are placed in the DDN. The DDN STF should also be used to conduct acceptance testing on vendor supplied components as a condition of government acceptance. The DDN STF is used to simulate the DDN environment and provide controlled operational conditions defined by relevant specifications. Acceptance requirements are also defined by relevant specifications.

2.1.1.1 Component Testing. Any DDN component should be capable of being tested in the STF, this testing may be either government acceptance testing or operational tests. The component should be capable of being tested in a standalone as well as a test bed network mode. This type of testing is a complete functional test of the component. Prior to the STF testing, testing at the vendor's site has been accomplished to ensure component integrity.

2.1.1.1.1 Hardware Testing. Government acceptance testing should be accomplished at the DDN STF. Routine acceptance testing is conducted to ensure contractor compliance with the equipment specification. Testing normally consists of workmanship and operating checks, as defined in Section 4 of the equipment specifications or in the contract and SOW for the items of equipment. Although this testing is not normally administered to all of the equipment, there is enough testing of hardware and associated software that the capability should exist at a government test facility.

2.1.1.1.2 Software Testing. The ability to test the performance and efficiency characteristics of a complete software implementation is complex and difficult to simulate in a network environment.

(a) One objective of software testing is to promote enhancement and maintenance of software for operational release by:

(1) Software release development and developmental testing
(2) Formal release testing
(3) Maintenance analysis, patch development, and patch testing
(4) Acceptance testing.

(b) Component testing of software is also necessary for:

(1) Development and adaptation of advanced software for experimental DDN use
(2) Investigation of feasibility and applicability of advanced software and its relationship to hardware in simulated subnetwork operational environment.

(c) All implementations of host interfaces to be connected to DDN require DDN PMO certification prior to operating on the network. Software testing at the component level should be initially directed toward:

(1) 1822 TCP/IP assistance
(2) Interoperability of 1822 vs X.25
(3) X.25 implementation testing
(4) TCP/IP validation testing.

2.1.1.1.3 IVV&T. The STF should be capable of standalone component testing during which IVV&T (government or contractor) may be conducted.

2.1.1.1.4 Security Test & Evaluation (ST&E). Although security devices and mechanisms will have been extensively tested and will have been subjected to thorough IVV&T procedures, ST&E testing should be directed toward ensuring functionality of the components in the DDN environment.

2.1.1.2 Network Testing. As with component level testing, network testing must accommodate the concept of emulating a network (standalone) as well as functioning in any of the subnetworks as a participating node.

(a) The DDN testbed should support the following functions:

(1) Applications software development and testing for distributed network processing
(2) Network application development and developmental testing
(3) Formal testing of new network applications in simulated current operational environment
(4) Nondegradation testing of existing network applications with new system hardware and software releases
(5) Maintenance analysis, patch development, and patch testing for network applications
(6) Advancement of information technology in support of DDN
(7) Evaluation and enhancement of performance
(8) Development of computer and network performance evaluation tools and techniques
(9) Assistance to non-DDN development and testing.

(b) The testing path should include

(1) STF to the Experimental ARPANET
(2) STF to BBN through a 50 kbps landline
(3) STF to operating networks through the DDN Backbone.

2.1.1.2.1 Monitoring Center. The Monitoring Center will incorporate automatic fault/failure recognition, isolation, and correction. This function initiates programs and actions that localize faults/failures that may require repair at places other than the STF. During the initial setup of the DDN network (network operation, control, and support) one MC C/70 should be

collocated with the STF for ease of initial network integration and testing. This C/70 can also provide network operational backup control to the primary MC C/70 to be located at DCOAC.

(a) Circuit testing. Functions of the monitoring center include automatic fault/failure recognition, isolation and correction, as well as loopback initiation to pinpoint failures. Testing of operational trunklines is, therefore, a function of the MC, not the STF. Circuit testing should be routinely accomplished by the MC to measure performance standards.

(b) Other elements of the backbone should be tested in the test bed network prior to release to operational nets.

(c) Other MC functions include:

(1) Software debugging
(2) Network configuration monitoring and control
(3) Performance data collection
(4) Software maintenance and distribution
(5) Improvement of user procedures, network operational procedures, and support and maintenance procedures.

In order to provide the vendor with the capability to monitor and analyze key components and associated network development and performance testing to satisfy contract requirements, one resident MC C/70 will be connected from the vendor's site to a DDN STF C/30 switching node through a 50 Kbps landline. STF access by the vendor will be scheduled and coordinated through the DDN STF Test Director. Vendor accountability for network utilization in terms of origin, destination, cost, time, and other important items is a DDN requirement and will be accomplished by the MC.

2.1.1.2.2 Security Test and Evaluation (ST&E). In the simulated network environment of the STF, ST&E testing should be directed toward ensuring that the following services are reliable and consistent:

(a) Link encryption

(b) End-to-end encryption

(c) Community of interest separation

(d) Protection against penetration or alteration

(e) Misdelivery.

2.2 System Test Facility (STF) Configuration. The functional capabilities required of the STF were addressed in the preceding sections. The following sections discuss the equipment and configurations necessary to provide these capabilities. Conceptually, the STF provides integration of the DDN development and test facility and the DDN Monitoring Center by common communication technical control equipped with an assortment of data circuits, communication and cryptographic hardware, and test equipment. The STF should be able to operate in either an integrated network mode, or in a nonintegrated (standalone) network mode.

The STF should be a government-owned and -operated facility. This setup overcomes problems associated with acceptance testing (paragraphs 2.1.1 and 2.2.2) of a vendor's competitively procured hardware or software being tested in another vendor's facility, i.e., without the inherent difficulty of protecting vendor proprietary information while testing. Problems associated with security level testing are also minimized, since the STF must be able to test in an environment equivalent to the highest classification on the network.

Testing capabilities should include a DDN host or other device which can simulate, control, and emulate all operating network characteristics of a DDN host.

The vendor requires linkage to the DDN. The vendor will have controlled access to the DDN network, by way of a resident C/70 connected to one STF C/30 through a 50 Kbit landline, in order to receive information relating to problems associated with their components within DDN. This allows the vendor to be a DDN subscriber, under the control of the STF Test Director, to satisfy contract test requirements.

The STF requires linkage to the active DDN for participation as a test node in Network integration testing. Further, operating within a military network not only exposes the STF to required network disciplines, but also improves overall network monitoring and control.

2.2.1 Testbed Configuration Flexibility. The STF must comprise a test bed of equipment types and quantities that will allow flexibility in test configurations with the capabilities for reconfiguration on a timely basis to meet changing test requirements. The requirement that results in most equipment is for the STF to be configurable as a standalone network. It is also stressed, however, that the DDN STF have a suite of equipment that will allow a number of test configurations simultaneously. One representative example would be a setup that requires three (3) STF C/30 switching nodes and all associated operational and test equipment in a DDN standalone test configuration to evaluate progressive versions of network TCP/IP protocol efficiency and robustness or IPLI and DES performance. Simultaneously, the STF is required to participate as a single node or multiple nodes to interact with an operational site during site transition, and also as a single node or multiple nodes with subnetworks during network integration. Within these configurations, there should be sufficient elements of each equipment type to be able to duplicate, as much as practicable, complex interactions and effects to verify functions and stress performance characteristics. Simulations may replace some of the more substantial equipment types, since it is not practical, nor cost effective, to have one of each of the many types of host available at the STF. Nevertheless, it will be possible to install and test actual operational equipment, regardless of type, at the STF prior to delivery and installation in the field.

2.2.2 STF Equipment. The type and quantity of STF operational and test equipment that will provide a flexible test bed are presented in Table 2-1. Two examples of the many possible

configurations available are provided in system block diagrams in Figures 2-2 and 2-3. The first is a standalone inter-subnetwork (Classified and Unclassified) integration test bed. The second is an intra-subnetwork (TS) test bed configuration in which STF participates in a minimal manner as one node with two (2) operational sites in transition. During site transition and network integration, the STF will serve as one node, at a minimum, and can be configured to participate with up to a maximum of five nodes. The equipment required in the minimum configuration is a subset of the network standalone configuration and will consequently require less equipment.

One example of testing that can be conducted utilizing the standalone configuration of Figure 2-2 is intersubnetwork adaptive routing. In the test setup, a simulated operational data transmission environment will be established for the classified subnetwork and the unclassified subnetwork, separately. At this point, each subnetwork is operating independently. Once the functions and performance for each are established, the classified subnetwork data will be routed through a gateway to the C/30 switching nodes of the unclassified subnetwork and back again through the other gateway to the classified subnetwork. This method of testing can be conducted to verify the following:

(a) Gateway functions and performance characteristics are in accordance with specifications.

(b) C/30 switching nodes can be shared in an adaptive manner by subnetworks of different classification levels without compromise or contamination of the data or security of either.

(c) IPLIs do, indeed, function and perform in accordance with specifications to isolate different Communities of Interest (COIs).

2.2.2.1 STF Subnetwork Traffic Generator. The STF test set would provide an "off-line" means of validation of any of the protocols at any level for any equipment, system, subsystem,

Table 2-1. DDN STF Equipment Types and Quantities

Network Operational Equipment Type	Quantity
C/30 Switching Nodes	5
Gateways	2
Hosts	*
Internet Private Line Interfaces (IPLIs)	5
Host Front End Processors (HFEPs)	*
KG84s	10
Data Encryption Standard (DES) Devices	10
Terminal Access Controllers (TACs)	2
C/70 Monitoring Center Devices (each w/3 terminals w/CRTs)	2
Mini-Terminals Access Controllers (Mini-TACs) (as available, will replace TACs)	2
Trunk Lines (full duplex capable w/adapters and connectors)	10
Modems (each type anticipated)	2
Multiplexers	*
Terminals (each type anticipated w/CRT, in addition to C/70 requirements)	1
Breakout Boxes (for RS-449/RS-232)	3
Hard Copy Terminal	1
Terminal Emulation Processors (TEPs)	*
Racks for All Equipment	
Resident Software for All Equipment	

Test Equipment	Quantity
Satellite Delay Simulator (full duplex, wideband capable)	1
Satellite Error Simulator (full duplex, wideband capable)	1
Terrestrial Link Delay Simulator (full duplex, wideband capable)	1
Terrestrial Link Error Simulator (full duplex, wideband capable)	1
Logic Analyzer	1
Subnetwork Variable Traffic Generator/Simulator/ Protocol Analyzer	1
Portable Subnetwork Traffic Generator/ Simulator/Protocol Analyzer	1
Line Monitors	3
Bit Error Rate Testers	2
Oscilloscopes	2
Program writer (for writing test routines onto disc/cassette/magnetic tape)	1
Patch panel	1

* As Required.

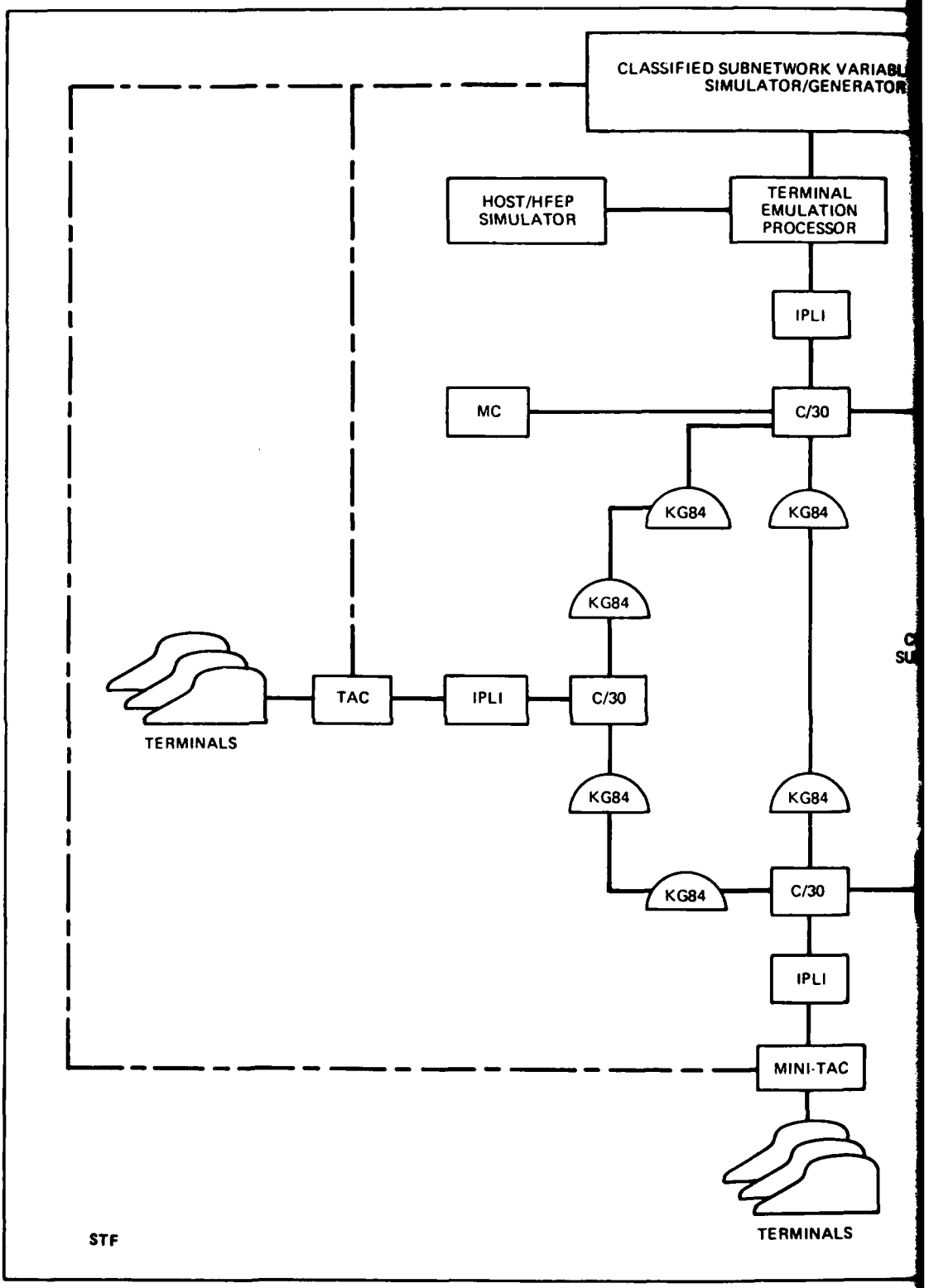
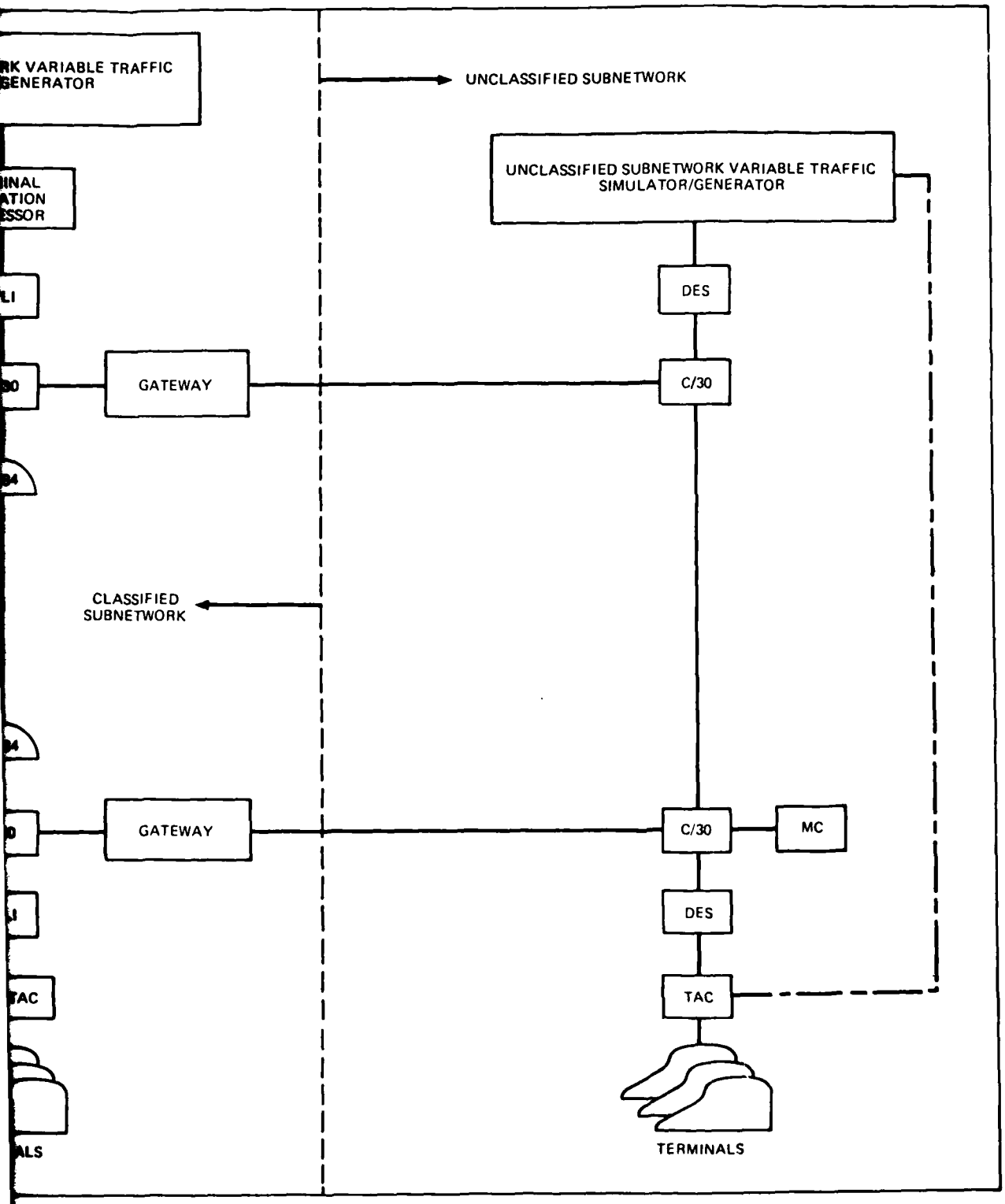


Figure 2-2. Sample STF Test C



TP No. 093-11160-B

Test Configuration for Network Standalone

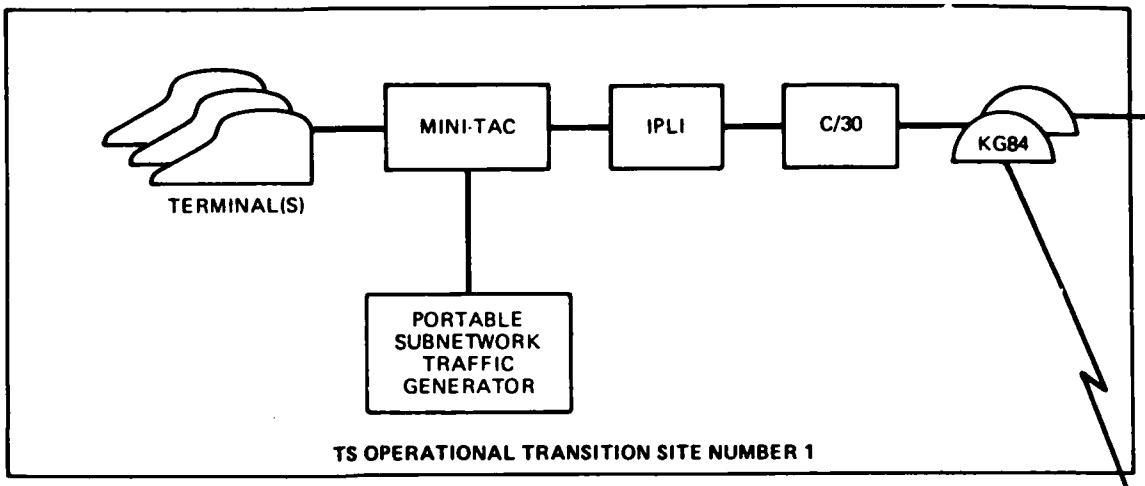
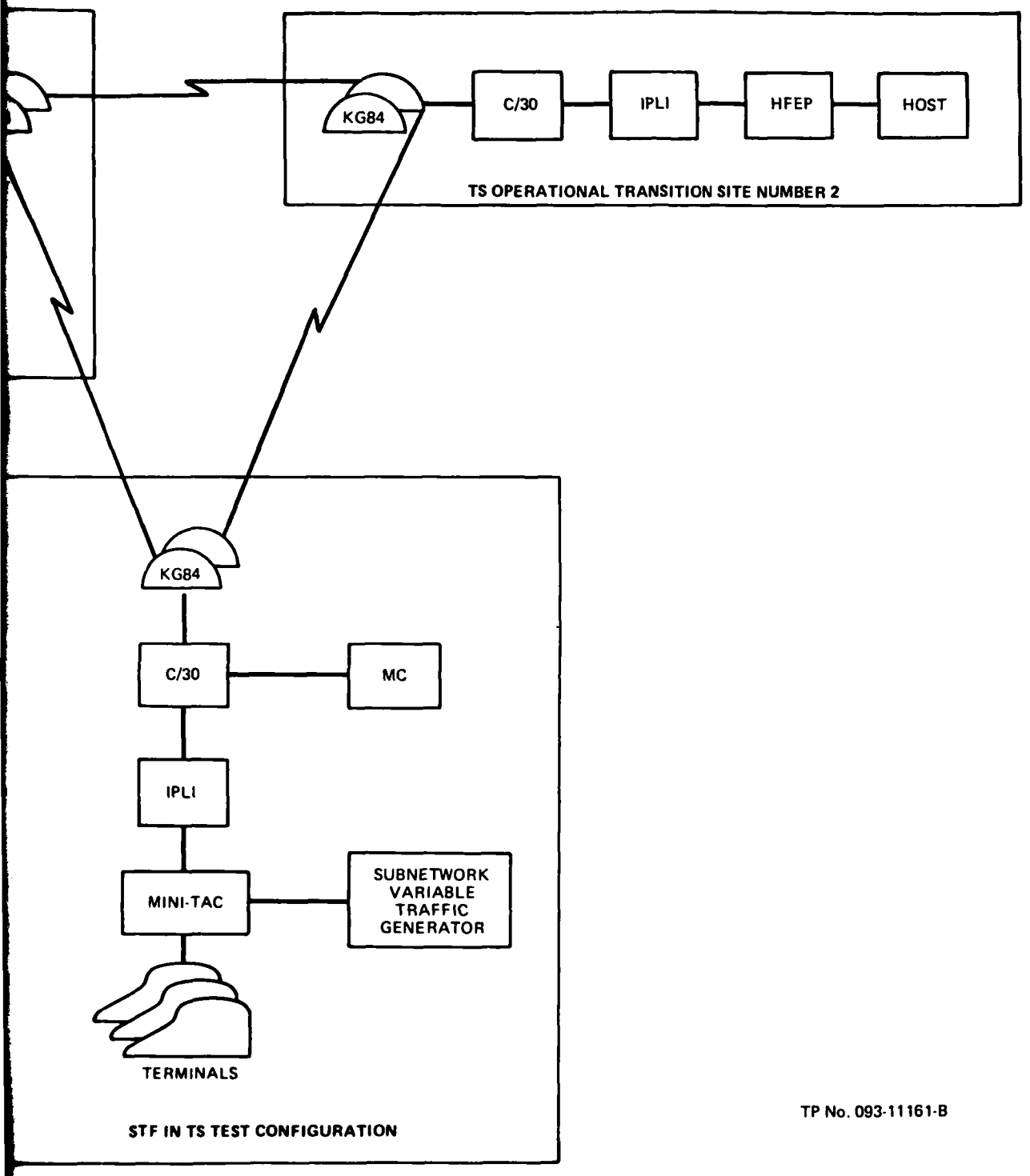


Figure 2-3. Sample Test C
as One Nod



TP No. 093-11161-B

e Test Configuration for STF
One Node in Site Transition

network, or subnetwork. Functional performance, as well as performance characteristics like robustness and efficiency could be verified. The capability to operate this test set remotely from a vendor facility or operational site is recommended, reducing the amount of travel required in testing/retesting and allowing for more unrestricted test time to be made available to increase confidence in the equipment under test. IVV&T of higher level protocols could also be performed in the STF using the STF test set. All protocol levels referenced in this Subtask are those defined by the seven-tiered ISO OSI model. They are provided for clarification, with examples, as follows:

(a) Level 1 - the physical layer (e.g., electrical IAW MILSTD 188C)

(b) Level 2 - the data link layer (e.g., HDLC IB and IIA)

(c) Level 3 - the network connection layer (e.g., 1822)

(d) Level 4 - the transport layer (e.g., TCP/IP)

(e) Level 5 - the session layer (e.g., Telnet O/C)

(f) Level 6 - the presentation layer (e.g., Telnet NVT)

(g) Level 7 - the application layer (e.g., User provided).

The STF subnetwork variable traffic generator/simulator/protocol analyzer referenced in Table 2-1 should be capable of the following:

(a) Generation/simulation of subnetwork traffic under test at levels 1 through 7 for X.25, IP, TCP, and all remaining protocols and applications at the highest stress levels practicable.

(b) Interrogation and analysis of vendor, site, and STF equipment protocols at levels practicable to verify functional, operational and performance integrity of protocols at stress levels required.

(c) Communication with the portable subnetwork traffic generator/simulator/protocol analyzer and all sites and vendors.

The capabilities described above may be accomplished by the current WIN Remote Terminal Emulator or a similar device.

2.2.2.2 Portable Subnetwork Traffic Generator. The Portable Test Set (PTS) referenced in Table 2-1 would provide a convenient and "off-line" means of verifying the functional integrity of lower level protocols at any interface of the equipment, whether at a vendor's site in acceptance testing, or at an operational site. Its use at operational sites may be particularly important in the preliminary, formative stages to provide user confidence that the site is operating correctly within itself prior to network entry. The PTS could also be used as a primary tool in the IVV&T phase. Further, a capability for the PTS to communicate with the STF for subsequent analysis is recommended.

The portable subnetwork traffic generator/simulator/protocol analyzer referenced in Table 2-1 should be capable of the following:

(a) Generation/simulation of subnetwork traffic under test sufficient for functional testing of X.25 levels 1, 2, and 3, and IP at level 3(c).

(b) Interrogation and analysis of vendor, site, and STF equipment protocols to verify functional and operational performance of X.25 at levels 1, 2, and 3, and IP at level 3(c).

(c) Transportability to any vendor, site, or to the STF as the situation dictates.

(d) Communication with the STF subnetwork traffic generator/simulator/protocol analyzer.

An early WIN RTE may perform the above functions.

2.2.3 Monitoring Center Configuration. The Monitoring Center (MC) will provide the equipment necessary to evaluate the performance and isolate faults in the backbone communications, the individual sites during and after transition, and the integrated

DDN. The equipment required to accomplish this will consist mainly of two (2) C/70 computer systems. One will run the current version of the NU software that provides summary information on network usage, availability and reliability. NU also provides tools for isolating failures in the network and for installing new software, and testing both the communications software and subscriber's application software. NU aids in software configuration management and provides remote tools for checking out field fixes to hardware.

The other C/70 will be used as a test bed for software evolutions as well as a backup for the primary MC C/70. Each C/70 will separately monitor both red and black performance. The physical connection of the C/70 will be to one or a number of the C/30 switching nodes in the STF or at the operational sites, as required. Three terminals with CRTs will be attached to each C/70 to allow sufficient access on the working level and to maintain adequate network control.

The system block diagram configuration for the MC is presented in Figure 2-4. This configuration will remain the same for all STF configurations, though it may be connected to different C/30 switching nodes both inside the STF, at the operational sites, or at the vendor(s) as the situation dictates.

It is important to note that the cryptographic isolation of the various internet communities in the DDN, although necessary because of security considerations, places constraints on the design of the monitoring and control facilities for the system. Since messages cannot pass the IPLI boundary without being encrypted in a manner consistent with the subnetwork classification, each community will require its own monitoring and control system. The effect of this requirement on the design of the MC attached to the STF will be one of two results. Either the MC will require multiple IPLIs keyable to each subnetwork for universal capability or the MC will only be able to perform its functions in support of one subnetwork, to be determined, with one keyable IPLI.

2.2.4 Security Configuration. Installation of TEMPEST compliant equipment in the STF must be accomplished in accordance with MIL-HDBK-232. End-to-end security test and evaluation must be done in accordance with the current version of DCA circular 370-D195-2.

Security requirements for the STF will be consistent with the classification of the highest level of facility resident data and equipment. Also, the DDN Security Architecture Review of 4 November 1982 identifies several options, or levels, of security that will, when selected, further shape the precise requirements for the facility. Nevertheless, a minimum set of facility requirements for the STF can be identified as follows:

(a) All switches, unclassified community IPLIs, trunk KGs, and the System Regional, Mobile, and unclassified Community MCs and the Software and Hardware Configuration Control Facilities are at restricted access locations designed to handle information in accordance with the security classification requirements of the service or agency responsible for the protection of the location. Personnel at these locations are required to have clearances consistent with these requirements.

(b) No specific protection requirements exist for modems and transmission media making up the trunks of link encrypted access lines, unconstrained access to such media must be assumed. Subscriber access area equipment (hosts, terminals, HFEPs, mini-TACs, TEPs, IPLIs for SECRET and above subscribers, and Community MCs) will be physically protected at the appropriate level for the plain text traffic contained in them. There are no restrictions on the locations of and personnel access to unclassified access area equipment, except as provided for in the governing service/agency regulations.

(c) No specific equipment for security test and evaluation has been identified as a permanent requirement for the STF. Analysis of data in the security testing identified in Subtask 1 using the operational equipment identified in Section 2.2.2 of this Subtask will yield adequate information to validate security functions. Selection of one of the options in the DDN Security Architecture Review may result in a requirement for additional equipment or measures and will be established as requirements become more refined.

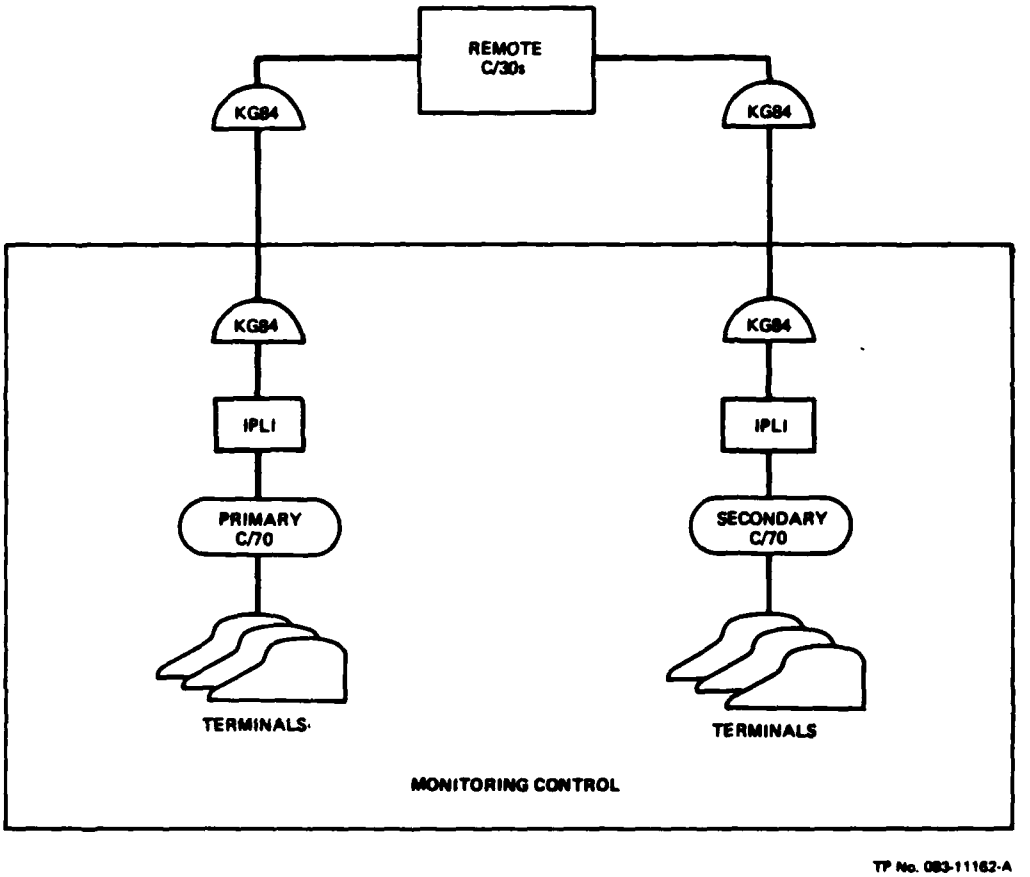


Figure 2-4. Monitoring Center Test Configuration

3. TEST MANAGEMENT

3.1 Organization Responsibilities. Section 3 of the DDN Management Engineering Plan specifies the organizational responsibilities for program management.

The DDN PMO is responsible for overall management of the DDN program, including test and evaluation of network components, standards and procedures for system operation, installation of network elements, activation and deactivation of DDN DCS trunks, and other elements which have varying degrees of impact on test and evaluation of DDN components. To ensure that the test and evaluation requirements are satisfied, the DDN PMO has established the Test and Evaluation Division.

3.2 The DDN System Test Director Responsibilities. The direction, planning, and management of the test and evaluation program will be accomplished by the DDN System Test Director (DDN STD) and supporting staff. The DDN STD and staff are responsible for the coordination and execution of network integration testing required of DDN subscribers. This responsibility includes the requirement to establish a capability for the STF to participate as a node in site transition and network integration testing prior to cutover to an operational DDN network. This responsibility also includes the requirement to establish the capability to independently validate performance characteristics of the hardware and software components and the integrated network required for DDN network operations, as well as to explore network enhancements. The STD will also be responsible for accountability of DDN network utilization statistics and the corresponding billing to users. Users will be charged for network services by system hook-up and number of packets sent through the system. These utilization statistics are resident in the STF MC C/70 NU software capabilities. It will be the responsibility of the DDN STD to access these statistics on a regularly scheduled basis, as determined by the DDN PMO, to apply the associated rates, and to charge back these costs to the design users.

To enhance communications and coordination among the operational and emerging networks, a DDN Test Planning Working Group (with a functional charter) chaired by a Network Integration Test Coordinator (NITC) should be formed. This group should assist the DDN STD in the overall scheduling and coordination of integrating networks into the DDN. Figure 3-1 displays the proposed organization.

The DDN STD has overall responsibility for conducting all required testing. He submits final decisions, based upon the findings and recommendations of the test team members, to ensure resolution of problems which might prevent the successful integration testing of the DDN. Staffing of the system test team, as described below, will be sufficiently broad to cover major functional test responsibilities.

3.2.1 System Test Facility Director (STFD). The STF Director reports directly to the System Test Director and supports him in his official capacity on all matters related to the STF activities. He directs the STF, resolves scheduling conflicts and ensures a complete set of test data, appropriate problem documentation, and proper configuration control. He is responsible for day-to-day operation and management of the portion of the STF that operates as part of the DDN, as well as allocation of assets required for developmental testing.

3.2.1.1 Software Support Engineer (SSE). The SSE at the STF will monitor all proposed software changes and identify possible impact on current system performance and prior testing. He will ensure that the software baseline, established at the beginning of acceptance testing, is controlled by configuration management throughout system testing. He will work with test team members to resolve software problem areas. He will assist the STFD in fulfilling his responsibilities. The SSE will work with the System Security Representative in documenting any malfunctions which may have an impact on the security design.

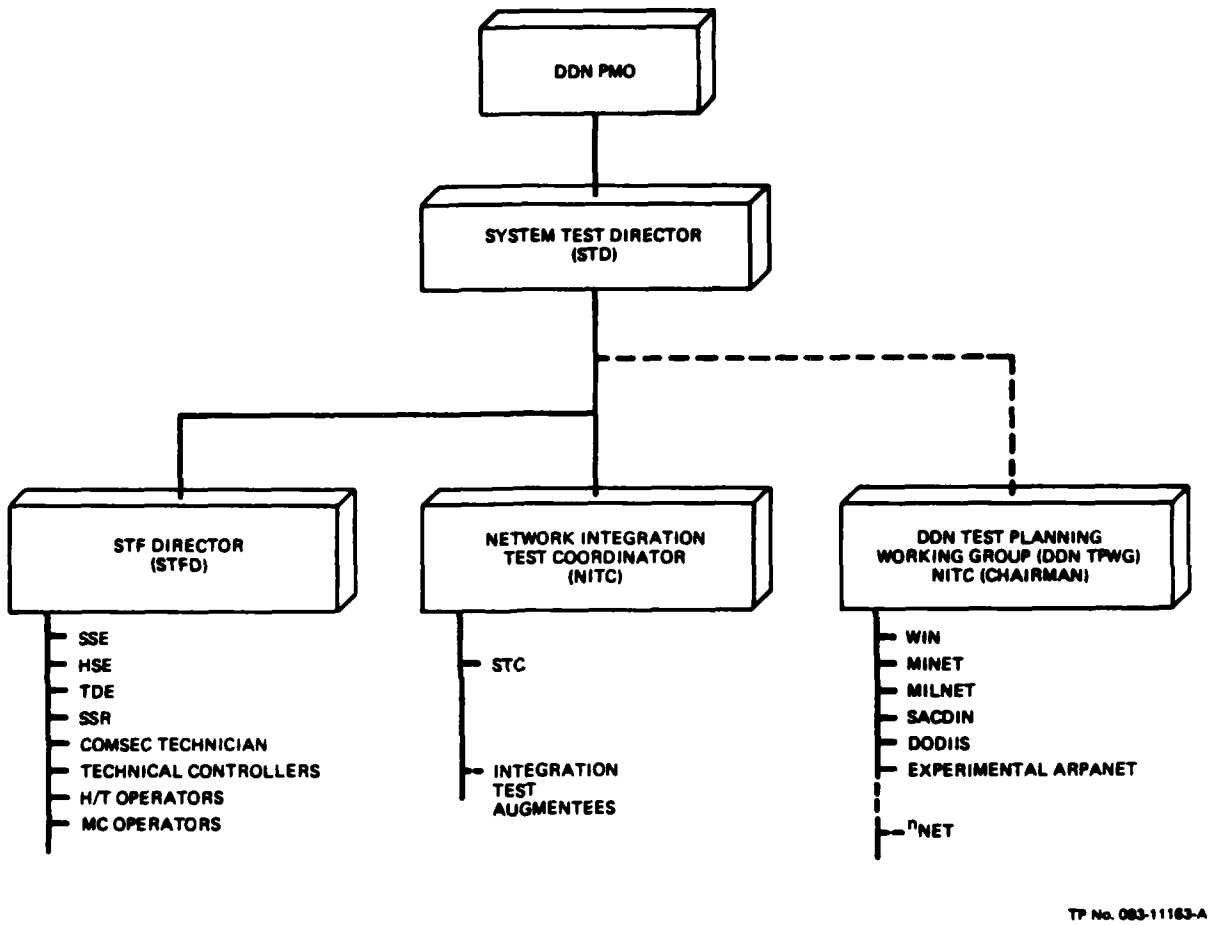


Figure 3-1. DDN System Test Organization

3.2.1.2 Hardware Support Engineer (HSE). The HSE will track all prepared hardware changes and possible impacts on system performance and prior test results. He will ensure that the hardware baseline, established at the beginning of acceptance testing, is controlled by configuration management throughout system testing. He will work with test team members and contractor personnel in resolving hardware problem areas. He will assist the STFD in fulfilling his responsibilities. The HSE will work with the System Security Representative in documenting any malfunctions which may have an impact on security design. He will assist in witnessing tests when required.

3.2.1.3 Test Design Engineer (TDE). The TDE will provide expertise in the design of tests to ensure that they will accomplish their intended purpose. He will provide technical advice and assistance to the STFD, the Network Integration Test Coordinator (NITC), and the Director of specific tests conducted at the STF in preparation of test plans, procedures, and scenarios; in the conduct of testing; and in the interpretation and analysis of test results with appropriate statistical and other measures.

3.2.1.4 System Security Representative (SSR). The SSR advises the STFD and provides security guidance related to vulnerabilities of and threats to the STF and security considerations prior to each test. He coordinates with the DDN PMO System Security Engineering Manager and Subnetwork Security personnel to identify specific system threats. The SSR ensures that the STF has proper physical security protective measures and that personnel security methods and procedures are commensurate with the various levels of classification and access required for testing. The SSR will witness all tests impacting on security considerations to make sure they are conducted as planned. The SSR will document all malfunctions that impact security during testing. He will be familiar with system operation and monitor all testing failures and configuration changes to assess their

security impact. He will work with other test team members and contractor personnel in resolving security-related problems. He will assist the STFD in documenting and reporting security-related problems. The SSR will ensure that security requirements of the specification are fully met and tested.

3.2.1.5 COMSEC Technician. The COMSEC Technician will perform technical duties required to support existing or developed cryptographic equipment and secure circuits. He will work with the SSR to ensure the necessary security environment exists to protect cryptographic resources.

3.2.1.6 Technical Controllers. Technical Controllers will be provided to both the STF and the Monitoring Center (MC). The controllers will man their normally assigned positions during the tests and become familiar with the operating procedures prescribed for the node or subsystem. If located at a field test site, they will respond to the STFD or the subnetwork test coordinators.

3.2.1.7 MC Operators. Operators will be familiar with the test objectives, the emergency procedures, and the operating functions of the Monitoring Center. They will man their normally assigned positions during tests. Operators will respond to direction from the STFD in performing test procedures.

3.2.1.8 STF Host/Terminal Operators. Host/Terminal Operators may be either permanently assigned to the STF or augmentees provided on a temporary basis, as coordinated by the DDN Test Planning Working Group. The operators must be thoroughly familiar with operating procedures and system requirements of the subnetwork they represent in the test procedure.

3.2.2 Network Integration Test Coordinator (NITC). The NITC will chair the DDN Test Planning Working Group. He will report to the DDN STD and will be responsible for coordinating all activities related to the integration testing of the various subnetworks prior to operational hookup to the DDN. The NITC, in coordination with the Subnetwork Specific Test Director, will

review integration planning, arrange schedules with the STFD, and ensure that any required subnetwork hardware, software, or other equipment is provided on a timely basis.

3.2.2.1 DDN Subnetwork Test Coordinators (STCs). Subnetwork Test Coordinators will be designated for the integration of each subnetwork into the DDN. The STC will be the DDN on-site representative for testing related to the integration of each node or subscriber system. Nodal integration is an activity of the DDN Backbone development and expansion. As such the STC will take the lead in coordinating, conducting and reporting test activities. Subscriber system integration is a function of the specific subnetwork PMO. The STC will coordinate with an appropriate subnetwork counterpart and the NITC. Once subnetwork activities begin the STC is authorized to contact the STFD directly to ensure successful accomplishment of test requirements.

3.2.2.2 Integration Test Augmentation. Subnetwork PMOs may provide subsystem specific technical personnel, operators and observers at the STF as required to accomplish test requirements.

3.3 DDN Test Planning Working Group (TPWG). The Test Planning Working Group is an organization made up of representatives of the DDN PMO and the Subnetwork Program Management Offices. The DDN TPWG will provide coordination of test planning and execution, and will confer with the DDN Test Director and Program Manager. The DDN TPWP will be chaired by the NITC during all phases of the test program, and will include representatives from each of the Subnetwork Program Management Offices.

The Test Planning Working Group will provide guidance and coordination on test-related activities and documentation, including: (a) Recommending or taking appropriate action on test-related problems, (b) Advising and assisting the Program Manager with the evaluation of new requirements generated during the course of testing, (c) Reviewing test planning documentation and providing inputs to applicable sections of those documents,

(d) Planning and coordinating of test resources and requirements,
(e) Making available the expertise of recognized technical advisors and specialists from their respective organizations.

The NITC will call meetings quarterly. TPWG subworking groups may meet more often as required as each subnetwork prepares to join the DDN.

4. TEST FACILITIES ACQUISITION

The acquisition of testing capabilities and support facilities falls under the Management Engineering Plan precept that the DDN program can be considered a modernization and expansion program. Testing of the DDN must take into account the baseline of existing networks and their respective test facilities. Test capabilities should begin with an initial capability and expand in a timely manner to fully support the evolution of the network through standalone testing and by acting as a node in any subnetwork undergoing integration.

4.1 Acceptance Test Capabilities. Acceptance testing is typically associated with testing at the Component Level (see 2.1.1). Government involvement in component testing may begin early in the development stage as warranted by the relative complexity of the desired end product.

4.1.1 Contractor Facilities. The evolution of the DDN is possible because a solid base of components is totally or nearly developed to operational standards. Key components, such as C/30 nodes and IPLI security devices still require considerable development and subsequent testing. Testing in various contractor facilities should follow normal contractual procedures to ensure that developed products meet contract specifications. Typical practices may include a network development laboratory and essential acceptance procedures wherein a specified prototype component is turned over to the government for a limited period to validate specifications and demonstrate preliminary component performance. In order to increase credibility of testing results, government testing at contractor facilities should be eliminated.

4.1.2. IVV&T CAPABILITIES. Those components requiring IVV&T will require testing facilities available to both government personnel and the designated IVV&T contractor personnel. The designated IVV&T contractor may conduct certain IVV&T activities at its own facilities. This activity could be

aided if the IVV&T contractor resources included on-site access to the Expermimental ARPANET. At a miniumum, a government facility with this capability should provide the required access for independent review.

4.1.3 Government Facilities. An initial test capability at a government facility is necessary to support the latter stages of Development Test and Evaluation or Category I testing, as suggested by DoD 5000.3. This is potentially the first time that all component elements (hardware and software) are integrated into a network. Facilities, equipment, and staff to support DT&E capabilities should be provided by Research and Development Funds. A key factor influencing testing at this juncture is the imposition of military-type discipline on network development.

Although testing may be supported or accomplished by contractor personnel, procedures and load factors must reflect expected operational requirements. The various host and related sub-network hardware and software are thoroughly tested to ensure a stable platform. Secondly, basic network user functions are tested to confirm that the system operates in accordance with design specifications. A host wraparound capability is an essential tool, stimulating, within the host, the functions of all network activities, including anticipated network responses. Acquisition of initial government test capabilities should begin early. Hardware, software, and test procedures must be subject to various acceptance evaluation measures in order to establish a known baseline to measure component and system criteria.

4.2 System Test Facility (STF). The primary focus in government test activity will be the DDN System Test Facility. The functional capabilities of this site will provide the initial baseline data necessary to integrate a successful network. The STF should have the organization, direction, and flexible component mix to emulate various configurations that will form the DDN. The STF will consist of a test bed capable of various

configurations, a monitoring center, and various supporting facilities to test the network.

4.2.1 DDN Test Bed.

4.2.1.1 Preliminary Test Bed Configuration. The test bed configuration for the stand-alone STF described in Section 2.1.2.1 is predicated on the availability of the equipment defined in Table 4-1. It should be noted that the full configuration for STF will not be realized for some time. The IPLIs, for example, are integral to a full functioning STF, but preproduction units will not be available until at least the third quarter of FY 84. A preliminary testbed, however, will be required to test some of the earlier integration efforts, for example, MINET integration into MILNET. The types and quantities of equipment that will be required to provide a flexible preliminary test bed configuration for this early effort are presented in Table 4-2. The equipment marked with an asterisk in this table is currently available at the Experimental Data Network at DCEC. It should be noted that, with minor exceptions, the preliminary test bed essentially exists for STF at the EDN. The notable exception is the DDN version of protocols required. Integrated testing involving classified nets must be withheld, however, until the arrival of the prototype IPLIs. In the initial configuration it is recommended that a monitoring center be located with the test bed. A C/70 is projected to be provided to the EDN by September 1983. Having the MC with the test bed will aid in the development of appropriate testing and controls without interfering with operational requirements of the DCAOC.

4.2.1.2 Enhanced Testbed Configuration. Enhancement of the test bed should be paced by the integration/transition schedules. Each enhancement should meet the specific expected requirements of the programmed tests and sub-network nodal or site configurations. Specific component mixes should surface in test planning by the DDN TPWG. The first enhancement of the test bed configuration should occur by the end of the first quarter FY 85 in preparation for MINET integration with MILNET.

Development and testing of the Secret Net should provide the next logical enhancement. Although WIN, DODIIS, and SACDIN will have a longer operational history, security considerations associated with the integration of the secret level net should be more feasible in promoting subscriber confidence. The insertion of secret data (real or simulated) will require the C/30 nodes to be placed in areas that are approved for handling and storing data that is classified at least at the secret level.

Components for a fully enhanced test bed may be allocated from contractual deliverables either as prototypes or initial production models. A fully enhanced test bed should include the minimum number of components listed in Table 4-2, many of these components are available in the EDN. Other components are located in the WIN test bed at CCTC and, with proper coordination by the NITC and the DDN TPWG, may be made available. Prototype or production IPLIs should be acquired in planned procurement actions.

4.2.2 Monitoring Center. The functional role of the Monitoring Center in test and evaluation is described in Section 2.2.3. It was previously recommended that the MC, at least initially, be located in the STF. The acquisition of the MC located in the DCAOC is provided for in planned procurement actions. The components located at the STF may be allocated from those destined for the CONUS based alternate MC.

4.2.3 Support Activities. The DDN test bed and MC must be linked to appropriate test equipment that would typically not be found at an operational node or subscriber site in order to provide realistic test environment and to accumulate measurable test data. A cable network and patchable jack field such as exists at the EDN is required to support the substantial flexibility of the test environments envisioned for the DDN. Test equipment such as that in the RCTF is required to inject delays, errors, and variable traffic loads; test measurement equipment is required to provide a means of monitoring and recording test

Table 4-1. Preliminary STF Test Bed Components

Component Type	Quantity
C/30 Switching Nodes *	3
PDP 11/70 Gateway *	1
VAX 11/780 Host *	1
Host Front End Processor	1
Terminal Access Controller *	1
DES Encryption Devices	10
C/70 Monitoring Center Devices *	1
3 terminals and CRT	
Trunk Lines *	6
Modems *	6
Breakout Boxes *	2
Terminal Emulation Processor (TED)	1
Terminal & CRT *	1
Hard Copy Terminal *	1
Resident Software for all equipment as appropriate	

* available in the EDN at DCEC

Table 4-2. Enhanced STF Test Bed Components

Component Type	Presently at EDN	WIN Test Bed	Quantity Required
C/30 Switching Nodes	3	3 (plus 1 TEMPEST)	5
C/70 Gateway	1		2
Host (VAX 11/780 or other)	1		1
Host Front End Processor			1
Terminal access Controller	1		2
Mini-Tac			1
KG-84		(4 On order)	10
IPLI (Prototype)			5
C/70 Monitoring Center 3 terminal and CRT	1	1	1
Trunk Lines			10
Modems			10
Breakout Boxes			2
Terminal Emulation Processors			2

results. The functional type of equipment listed in Table 4-3 is considered essential and is presently available at the RCTF.

Certification of the various host implementations of X.25, IP, and TPC protocols requires the capability of testing both remotely at a vendor or operational site and at a fixed location. The projected DCEC/NBS protocol laboratory will provide this essential capability and should be developed at the earliest possible date.

Table 4-3. DDN STF Test and Monitoring Equipment

Test Equipment	Quantity
Satellite Delay Simulator (full duplex, wideband capable)	1
Satellite Error Simulator (full duplex, wideband capable)	1
Terrestrial Link Delay Simulator (full duplex, wideband capable)	1
Terrestrial Link Error Simulator (full duplex, wideband capable)	1
Logic Analyzer	1
Subnetwork Variable Traffic Generator/Simulator/ Protocol Analyzer	1
Portable Subnetwork Traffic Generator/ Simulator/Protocol Analyzer	1
Line Monitors	3
Bit Error Rate Testers	2
Oscilloscopes	2
Program writer (for writing test routines onto disc/cassette/magnetic tape)	1
Patch panel	1

5. ALTERNATIVES

5.1 General. It was determined from the testing and recommendations of Subtask 1 that a definite need exists for independent government testing of DDN components and the overall DDN network. Subtask 2 has defined potential STF equipment and configuration requirements, the following paragraphs summarize the test bed configuration acquisition recommendations contained in section 2 and 4 and discuss alternatives that are considered less responsive to DDN requirements.

5.2 Preferred DDN STF Configuration Summarized. Information provided throughout sections 2 and 4 of this report envision an evolving DDN STF in which there is a build-up of functional capabilities commensurate with subnetwork integration into DDN. This approach is based on the premise that the DDN PMO is going to have a fully capable and operational STF.

5.2.1 Location. As presently planned, the STF would be located at DCEC.

5.2.2 Test Bed. The test bed would evolve into a configuration as described in paragraph 2.2. Based on an analysis of subnetwork integration schedules and testing requirements, the time phasing of STF capabilities may be determined. The STF would be set up first in the standalone mode for developmental testing activities, then for network integration activities.

5.2.3 Testing Capabilities. As discussed in paragraph 2.1 and 2.2, the full range of testing capabilities is brought on-line in accordance with the DDN subnetwork integration schedule and security device availability.

5.3 Alternative 1. DDN Minimum Capability STF. In this alternative, the DDN PM would have to distribute DDN testing requirements among subnetwork test facilities, rely heavily on government oversight of vendor testing, and increase reliance on contracted independent testers.

5.3.1 Alternative Locations. The DDN minimum capability STF would more than likely become adjunct of regional MCs, deriving testing requirements from faults diagnosed by MCs. A small STF capable of some independent software maintenance and enhancement testing could be accomplished at the CODUS MC. The bulk of software testing would be independently contracted or assigned to subnetwork STFs.

5.3.1.1 Increased Vendor Testing Capabilities. Relative control and emphasis in the scope of test bed testing is possible based on the degree of trust and demonstrated security capabilities of major vendors. There are restrictions in the Government COMSEC Community which prohibit contractors from operating classified communications centers, nevertheless, a good portion of early testing may be considered development testing. A contractor who has configured his facility to meet required DoD security standards, including appropriate personnel security clearances and accesses, could be given the task of doing more extensive testing.

5.3.1.2 Vendor Testing in Government Facility. In the case of the current prime contractor, BBN, an alternative is to negotiate secure working space from Air Force Systems Command/Electronic Systems Division (AFSC/ESD) at Hanscom Field, Bedford, Massachusetts. This would provide a secure facility under military control in the immediate proximity of BBN's technical staff. In either of the above alternatives, it may be desirable to allow at least a classified node test capability for participation with the STF during acceptance testing or to interact with the STF for more ambitious, higher level network protocol testing. This participation would be as directed by the PMO. The involved vendor would be responsible for funding this capability through research and development contract modifications.

5.3.1.3 Alternate Government Facilities. A service may be willing to accept responsibility for test and evaluation of the DDN. The Air Force, for example, could use its test environment at the Air Force Operational Test and Evaluation Center (AFOTEC), Kirtland AFB, New Mexico. The Army and Navy would have similar test facilities. Such an alternative would not significantly change the required component mix, but may resolve potential conflicts with projected programs at DCEC.

5.3.2 DDN Minimum Test Bed. The DDN test bed would be limited to the preliminary level described in paragraph 4.2.1.1. A configuration of three active C/30 switching nodes would scale down the number and types of additional network equipment required, thereby reducing cost of equipment and manpower. The capabilities of a three-node network are not fully understood. For example one of more critical and complex considerations in a "minimal" standalone capability is whether or not DDN subnetwork tests conducted at the DDN STF would produce significant results. A reasonable argument could be introduced implying that there is no significant degradation resulting in three-node versus five-node testing. This fact, coupled with the information that meaningful operational testing can only be executed on large operating networks could be used as argument for the minimum test bed configuration.

It can also be argued that serious limitations will result from a minimal test facility configuration, for example, the limited or potential nonavailability of STF resources to satisfy all required testing situations. Given a setup that requires a three-node configuration to develop or validate new software or software protocols would prohibit the three-node network from participating in a partitioned network test. Scheduling and overall coordination would be difficult, at best.

5.3.2.1 Use of Partitioned Subnetwork. The minimal test bed capability would necessitate a quicker introduction of the STF as an integrated operational test node to compensate for any loss of capability, yet provide adequate interaction and traffic loading.

Essentially, the minimal test bed would benefit from extensive interaction with the Experimental Arpanet for unclassified testing. There are, however, security liabilities in this arrangement; system capabilities and vulnerabilities may be revealed to non-DoD communities. The minimal test bed must be linked to a partitioned operational subnetwork to provide full test capability prior to that subnetwork's cutover to the DDN backbone. The availability of the partitioned network and disruption to normal operations is the limiting factor in this alternative. Extensive planning and coordination through the DDN TPWG would be required, but overall system capabilities and vulnerabilities may otherwise be revealed. When the minimal test bed is linked as a part of a partitioned operational subnetwork (experimental ARPANET) the availability of the partitioned network may be the limiting factor that would require extensive coordination through the DDN TPWG.

5.3.2.2 Increased Site Level Testing. Another economy of testing is to provide a sufficient number of portable protocol analyzers to allow flexible onsite testing of lower level protocols during site transition, thereby limiting the amount of STF involvement at the lower level. The STF would encompass more rigorous and concentrated testing at the DDN higher levels of network concern. The precise number of portable analyzers can be determined as schedules, and thereby usage requirements, are defined.

5.3.3 Testing Capabilities. The minimal test bed would necessarily reduce capabilities to either network participation or standalone testing, leaving the STF in the position of a software development laboratory incapable of simultaneous network interaction or integration.

5.3.3.1 Increased Commitment to IV&V. Test and evaluation is an essential element in software life cycle development, however, experience has shown that the thorough and accurate statement of specifications rigidly enforced during design and development can increase the prospects for successful programs and reduce the complexities and duration of test activities. A recognized tool to accomplish this procedure is Independent Verification and Validation and Testing (IVV&T) done by independent contractors at their facilities or at the STF. Program performance test plans are evaluated to ensure that the overall functional characteristics at all levels of operations are identified to certify that the software represents the system requirements. Software documentation and testing validation is performed to:

(a) Verify the total man-machine interface.

(b) Validate system initialization, data entries via peripheral devices, program loading, restarting, and the monitoring and control of system operation from display consoles and other stations, as applicable.

(c) Verify the interfacing of all equipment.

(d) Verify the capability of the program to satisfy all applicable system and program performance.

(e) Verify the capability of the program to operate at saturation levels which stress the software's capabilities in terms of response times and data handling capacity.

(f) Verify the capability of the systems to handle erroneous inputs properly, and to survive them.

(g) Verify inter- and intrasystem protocol formats and interfaces.

The entire IV&V process makes direct use of all contractually invoked references to MIL-STDs, DIDs, Directives, and Instructions.

5.4 Alternative 2. Immediate Setup of Entire DDN STF. The only differences between alternative 2 and 3 are initial costs and personnel requirements. Equipment listed in paragraph 2.2 would be required immediately (security devices, as available).

5.4.1 Location. As presently planned, the STF would be located at DCEC.

5.4.2 Test Bed. The test bed would become available immediately for the standalone mode. Software testing and enhancement testing could begin immediately without regard to subnetwork integration dates.

5.4.3 Testing Capabilities. As discussed in paragraphs 2.1 and 2.2, the full range of testing capabilities (except security devices) is immediately available for standalone testing and verification of software developments and protocols, eliminating total reliance on outside testing agencies.

5.5 Recommended DDN STF Configuration Alternative. The discussions to this point indicate that alternative 2 is the preferred alternative for the following reasons.

(a) A full capability DDN STF independent of other subnetwrok test facilities is required by the DDN PM in order to fulfill DDN testing responsibilities in the areas of component testing, network integration testing, IVV&T, and acceptance testing.

(b) A time-phased buildup of capabilities is the most cost-efficient method of STF acquisition in terms of capabilities required for subnetwork integration, and personnel required for STF operation.

(c) The acquisition and operation of a DDN STF reduces reliance on vendor testing. An efficient, disciplined STF also promotes confidence in test results.

APPENDIX A

LIST OF ACRONYMS

ARPA	Advanced Research Projects Agency
CDRL	Contractor Data Requirements List
DCA	Defense Communications Agency
DCS	Defense Communications System
DDN	Defense Data Network
DODIIS	Department of Defense Intelligence Information System
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
HFEP	Host Front End Processor
HIP	Host Interface Protocol
HSE	Hardware Support Engineer
IMP	Internet Message Processor
IP	Interface Protocol
IPLI	Internet Private Line Interface
IVV&T	Independent Verification, Validation and Test
MC	Monitoring Center
MILNET	Military Network
MINET	Movement Information Network
NITC	Network Integration Test Coordinator
PEM	Power and Equipment Monitor
PMO	Project Manager's Office
PS	Packet Switching
SACDIN	Strategic Air Command Data Information Network
SIP	Segment Interface Protocol
SOW	Statement of Work
SSE	System Support Engineers
SSR	System Security Representative
STC	Subnetwork Test Coordinator
ST&E	Software Test & Evaluation
STF	System Test Facility

STFD	System Test Facility Director
TAC	Terminal Access Controller
TCP	Transmission Control Protocol
T&E	Test & Evaluation
TEP	Terminal Emulation Processors
TEMP	Test and Evaluation Master Plan
WIN	WWMCCS Intercomputer Network